# New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector - Some Initial remarks

Louveaux, Sophie; Pérez Asinari, María Veroníca

*Published in:*
Computer and Telecommunications Law Review

*Publication date:*
2003

*Document Version*
Publisher's PDF, also known as Version of record

# New European Directive 2002/58 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector—Some Initial Remarks

SOPHIE LOUVEAUX* AND MARÍA VERÓNICA PÉREZ ASINARI**

## Introduction

The European Commission launched a review of the telecoms regulatory framework in 1999. The goals of the review were five-fold: to promote more effective competition; to react to technological and market developments; to remove unnecessary regulation and to simplify associated administrative procedures; to strengthen the internal market; and to protect consumers.[1]

One of the results is Directive 2002/58 on privacy and electronic communications,[2] which replaces Directive 97/66[3] concerning the processing of personal data and the protection of privacy in the telecommunications sector, in order to adapt it to new technology,[4] mainly to the internet.[5]

It constitutes a *lex specialis*[6] *vis-à-vis* Directive 95/46,[7] being also an instrument to avoid obstacles to the internal market,[8] facilitating its development.[9] The free flow of information is guaranteed through the harmonisation of the level of protection of privacy and personal data.[10] The new Directive expressly mentions the observation of the principles recognised by the Charter of fundamental rights of the European Union,[11] particularly Arts 7 and 8.

In this article we will refer briefly to some aspects of the new Directive: the services concerned, cookies, unsolicited communications, and traffic data.[12]

## Services Concerned

Article 3(1)states:

> "This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community."

* Former researcher at the *Centre de Recherches Informatique et Droit* (CRID), University of Namur, Belgium; co-founder of *e-consult, http://www.e-consult.be*. She can be contacted at sophie.louveaux@e-consult.be.

** Researcher at the *Centre de Recherches Informatique et Droit* (CRID), University of Namur, Belgium. She can be contacted at veronica.perez@fundp.ac.be.

We would like to thank Professor Yves Poullet and Jean-Marc Dinant for their valuable comments on this paper.

1 *The 1999 Communications Review*, European Commission, DG INFSO, Directorate A, September 2000.

2 Directive 2002/58 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] O.J. L201 ("the Directive").

3 Directive 97/66 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector; [1998] O.J. L024/1.

4 See: A. de Streel, R. Queck, and P. Vernet, "*Le nouveau cadre réglementaire européen des réseaux et services de communications électroniques*", in *Cahiers de droit européen*, 2002, No.3–4, 243–314.

5 Indeed, the principle to be followed is of "technological neutrality", which is crystallised in Recitals 4 and 46 of the Directive, and in general changes in the wording, for instance, "call" was replaced by "electronic communication". "*Ce principe vise tenir compte de la convergence et assure qu'aucune technologie n'est favorisée ou défavorisée par la réglementation. Ainsi, un service particulier doit être soumis au même régime, peu importe le type de réseau utilisé.*", in De Streel, Queck, Vernet, *op. cit.* Concerning the applicability of Directive 97/66 to the internet, the doctrine was pacific on this point. The Article 29 Working Party was also "for" this position ("Privacy on the Internet-An integrated EU Approach to On-line Data Protection", November 21, 2000, WP37). Moreover, Directive 2000/31 on electronic commerce explicitly recognises the applicability of the former Directive to information society services both in its preamble and provisions (Recitals 14 and 15, Arts 1(5)(b) and 8(2)).

6 Art.12 of the Directive. However, this Directive broadens the scope of Directive 95/46 to "provide protection of the legitimate interests of subscribers who are legal persons." It is not clear whether all the principles (rights and obligations) contained in Directive 95/46 would be applicable to legal persons acting as subscribers of electronic communication services, and what would be the extent of the concept "legitimate interest of legal persons", in the case the wording "legitimate interest" would reduce the protection given to natural persons.

7 Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] O.J. L281.

8 The legal basis is Art.95 of the TCE. See Recital 8 of the Directive ECT (European Communities Treaty).

9 "The successful cross-border development of these services [digital services] is partly dependent on the confidence of users that their privacy will not be at risk." Recital 5 of the Directive.

10 Art.11 of the Directive.

11 Full text of the Charter of fundamental Rights of the European Union, O.J C364/1, *http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf.*

12 We have developed an article-by-article analysis of the Proposal for the present Directive in S. Louveaux and M. V. Perez Asinari, *Proposal for a directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385*, written in the framework of the ECLIP project, available at *http://www.eclip.org/documentsII/sum/research.htm.*

The concept of "electronic communications services" is defined in Directive 2002/21 on a common framework for electronic communications networks and services[13]:

> [it is a] "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks."[14]

One of the typical services covered would be the one offered by the internet access provider. The word "normally", as concerns remuneration, is pertinent since Internet access can be provided for free. Indeed, in many of those cases it can be considered that the remuneration is indirect, since it is a third party, such as an advertiser, who pays the provider allowing the service to be given to the user for free.

Information society services are not completely excluded[15] from the scope of the Directive. Directive 98/48[16] amends Directive 98/34 and defines "information society service" as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[17]

For example, the "e-commerce" Directive 2000/31[18] describes the service provided by different intermediaries ("mere conduit", "caching", and "hosting"). "Hosting" consists of "the storage of information provided by a recipient of the service". At the internet service provider level (which hosts websites, when they are not "self-hosted" through the user-own servers), there is no transmission in a communication network of information or no "conveyance of signals on electronic communications networks". So, "hosting" is excluded from Directive 2002/21. The same reasoning could be applied to the web administrator.

Nevertheless, Directive 2002/58 uses a functional approach, and we have to consider other services or activities beyond those that would be "strictly" included in Art.3(1), mentioned both in the text of the instrument as well as in the Explanatory Memorandum.[19] There we find, for instance, reference to "unsolicited communications" or "cookies". Sending unsolicited electronic mail can be done, for instance, by a web-administrator using the data he has collected. Cookies are placed by web administrators or cyber-marketing companies. So, these activities are covered by the Directive to the extent that is mentioned in the text,[20] irrespectively of "who" does so (the question to answer is "what" any specific actor does in order to know if his activities fall under the Directive's regulations).

By speaking about "public available electronic communications" the Directive excludes the services provided within Closed Users Groups. So, the processing of personal data in this case would be regulated under the Directive 95/46. The Article 29 Data Protection Working Party criticises this decision because private networks are gaining an increasing importance in every day life and communications of citizens.[21]

The adverbial phrase of place "in the Community" used at the end of Article 3 (1 should be understood as qualifying the second part of the sentence, that is: "the provision of publicly available electronic communications services in public communications networks". We can imagine the example of the provision of one of these services from outside the Community to a subscriber or user located inside—or "in the Community"—(*e.g.* internet access). If we think about the applicable law to this situation that would be the case of Art.4(1)(c) of Directive 95/46,[22] since this service provider will use servers ("equipment") located inside the Community for purposes of processing personal data (*e.g.* "collection"[23] of IP addresses in the http logfiles). In those cases, it is clear that even through the applicable law rule contained in Directive 95/46, Directive 2002/58 would be applicable to the situation described above. If further processing of this personal data is intended to be done "outside" the Community, Arts 25 and 26 of Directive 95/46, would be of application.

## Cookies

The question of cookies is addressed in the Directive, both in the Recitals (24 and 25) and "implicitly" in Art. 5. Indeed the Directive aims at being technologically neutral and therefore speaks of "technical storage of information" or "access to information stored in terminal equipment".

After having stressed that terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private spheres of users requiring protection under the European Convention for Human Rights, the Recitals recognise that cookies may be a legitimate and useful tool for example in verifying the identity of users engaged in on-line transactions. In this sense, Art.5(3) limits the use of technical storage or access to information stored in terminal equipment for sole purpose of

13 Directive 2002/21 of the European Parliament and of the Council on a common framework for electronic communications networks and services. [2002] O.J. L108.

14 Art.2(c) of Directive 2002/21.

15 Art.5 3 of the Directive makes explicit reference to the provision of information society services (when technical storage or access—*e.g.* the case of cookies—is strictly necessary to provide an information society service explicitly requested by the subscriber or user).

16 Directive 98/48 of the European Parliament and of the Council amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. [1998 ] O.J. L217.

17 Art.1(2) of the Directive.

18 Directive 2000/31 of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. [2000] O.J. L178.

19 Indeed, we consider that this lack of clarity in Article 3 1 could have been amended adding "exceptions" to the principle expressed therein.

20 Even if they do not consist "wholly or mainly" in the conveyance of signals on electronic communications networks.

21 Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector COM (2000) 385. WP36. Working Party on the Protection of Individuals with regard to the Processing of Personal Data. available at *http//:europa.eu.int/Comm/internal_market/media/dataprot/wpdocs/wp36en.pdf*

22 Art.4. National law applicable: "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: ( . . . )(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.".

23 "Collection" is one of the actions contained in the definition of "processing" (Art.2(b) of Directive 95/46).

carrying out or facilitating the transmission of a communication over an electronic communications network or to facilitate the provision of information society services. For example, the use of a cookie in a website offering travel itineraries may help avoid that the user need to restate his town of departure for each connection.

It is interesting that on the subject of the legitimacy of cookies, the Directive does not make a distinction between permanent and session cookies. Indeed whereas permanent cookies remain on the terminal equipment after the closing of a connection, session cookies which may indeed in some cases be necessary for the functioning of the website, disappear at the end of the session. According to the Belgian data protection commission, whereas the use of session cookies may be considered in some cases as necessary and complying with the data protection principles, this is not always the case as regards the use of permanent cookies.[24]

Article 5(3) conditions the use of cookies to the provision of clear and precise information in accordance with Directive 95/46 about the purposes of the cookies or similar devices so as to ensure that users are made fully aware of the information being placed on the terminal that they are using.

Finally, Art.5(3) conditions the use of cookies to the possibility for the users to refuse to have a cookie or similar device stored on their terminal equipment. However the article implicitly admits that in the event that one refuses the placing of a cookie for a legitimate purpose, access to specific web site content may be refused. Indeed according to the terms of the Directive, the refusal:

> " . . . shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."

This position is contrary to that adopted by the Belgian data protection commission according to which the access to web site content may not be made conditional on the acceptance of a permanent cookie.[25] One may indeed question the legitimacy of such a practice : in an off-line world it would be like tagging each individual entering a shop, whether or not he merely enters for a few moments or decides to buy goods. If he refuses the tagging he would be refused the entrance into the shop. Can one still speak of the freedom of movement?

The information and right to refuse may be offered, according to the recital, once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or request consent should be made as user friendly as possible.

It is interesting to note that the Directive does not mention any limit as to the conservation period of the device. Indeed, in many cases cookies are placed on the user's terminal equipment, for very long periods of time, which seem to exceed those necessary to pursue the legitimate purpose (30–50 years). If one is to respect the provisions of Directive 95/46, these devices should only be placed on the terminal equipment only for as long as necessary to achieve the legitimate purpose.

24 *Avis* 34/2000 of November 22, 2000, see *www.privacy.fgov.be.*
25 *ibid.*

## Unsolicited Communications

Article 13 of Directive 2002/58 deals with the question of unsolicited communications. The idea is to provide safeguards for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, fax machines and emails including SMS messages.[26]

The regime which applies to these types of communications will depend on the means used to send the communication to the person targeted.

If communication means such as automated calling systems, e-mail, facsimile machines are used, then Art.13(1), (2) and (5) of Directive 2002/58 will apply (see below).

If other forms of communications means such as person-to-person voice telephony calls are used then Art.13(3) and (5) will apply (see below).

If other means are used such as postal mail, then Art.14 of the general Directive 95/46 applies. According to this article, the data subject has the right to object on request and free of charge, to the processing of personal data relating to him which the controller anticipated being processed for the purposes of direct marketing. This is called opt-out. The data subject is considered to have given his/her consent until he/she specifies otherwise.

Article 7 of the e-commerce Directive 2000/31 will apply if the unsolicited communication is provided within the frame of an "information society service" that is to say a service normally provided for remuneration at a distance by electronic means at the individual request of a recipient of services. According to this provision Member States which permit unsolicited commercial communications by electronic mail should ensure that such a commercial communication by a service provider established on their territory is clearly identified as soon as the communication is received by the recipient. It also provides that Member States ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect opt-out registers in which natural persons not wishing to receive such communications can register themselves.

The applicable regime will also vary according to whether or not the unsolicited communication is sent to a natural or legal person. Indeed, the general Directive 95/46 only affords protection to natural persons (Art.2 of the Directive). The Electronic Communications Directive which affords protection in principle to both legal and natural persons excludes, however, the application of Art.13 (1) and (3) to legal persons. This implies that legal persons will not be subject to an opt-in regime, but only to an opt-out regime.

Article 13(1) establishes the regime of opt-in whereby in principle the use of automated calling machines, fax machines and emails for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. Indeed it is believed that these forms of unsolicited commercial communications may, on the one hand, be relatively cheap and easy to send and, on the other, may impose burden and/or cost on the recipient. Moreover in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such reasons it is considered justified to require that prior explicit consent of the recipient is obtained before such communications are addressed to them.[27]

26 See Recital 40 of the Directive.
27 *ibid.*

However, Art.13(2) softens the regime for unsolicited electronic commercial communications sent within the framework of existing customer relationships. Indeed, it is believed that within the context of existing customer relationships it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the contact details according to Directive 95/46. When the contact details are obtained, the customer must be informed of their future use for direct marketing purposes in a clear and distinct manner and given the possibility to refuse such use free of charge. This possibility must be continued to be offered with each subsequent direct marketing message in the case the customer has not initially refused such use. One can question the impact of such a provision on the market in that it is favourable to large companies with pre-existing customer relationships.

For all other forms of unsolicited commercial communications by telecommunications means such as person-to-person voice telephony calls, Art.13(4) enables Member States to choose between an opt-in or opt-out regime. The idea is that since these forms of direct marketing are more costly for the sender and impose no financial cost on the receiver this may justify the maintenance of a system giving subscribers and users the possibility to indicate that they do not wish to receive such calls (opt-out). Nevertheless, in order not to decrease existing levels of privacy protection, Member States should be entitled to uphold national systems only allowing such calls to subscribers and users who have given their prior consent[28] (opt-in).

In all cases, Art.13(4) prohibits the sending of electronic mail for purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease. Indeed to ensure the effective enforcement of the rules on unsolicited commercial communications it is important to prevent the use of false identities or false return addresses.

## Traffic Data

### The concept of "traffic data"

"Traffic data" is defined as "any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."[29]

Directive 2002/58 foresees that interception or surveillance of communications and the related traffic data is prohibited, except when legally authorised in accordance with Art.15(1).[30] We have to remember that it is a legal principle to interpret exceptions restrictively.

The principle is that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.[31] Here again, without prejudice to Art.15(1), as well as Art.6(2) (billing purposes), Art.6(3) (marketing of electronic communications services or for the provision of value added services), and Art.6(5) (customer enquires, fraud detection, etc.).[32]

Traffic data are those data needed by the protocols to carry out the proper transmission from the sender to the recipient.[33] Traffic data consist partly of information supplied by the sender (*e.g.* email address of the recipient, URL) and partly of technical information generated automatically during the processing of an electronic communication (*e.g.* IP number,[34] routers, etc.). However, the extension of the concept of "traffic data" is not absolutely clear. Indeed, the extension of the concept needs to be de-limitated with precision since this data can be revealing of the activity carried out by the internet user, his contacts, preferences, characteristics, etc. Those data will generate more accurate personal descriptions if the concept of traffic data is enlarged, which could be a risk for the fundamental right of personal data protection.

The extension of the concept of "traffic data" is supposed to be determined by national regulations, even if this could generate different interpretations of the very concept of traffic data by the Member States, which could lead to certain obstacles in the internal market. This is because the obligation to store more data in one country than in other can create obstacles to the provision of services. Consumers would be more interested in using the service which respect more their privacy.

The concept of "data processed for billing purposes" does not present many problems.[35] In the context of the internet, less and less data is routinely kept for the unique purpose of billing. On the one hand, in the case of an access using a "pay per call" communication line (modem on an analogue phone line or Terminal Adaptor on a numeric [ISDN] line), the telecommunication operator needs to collect the date and time of the communication, its duration, the number called, and, of course, the calling number of his subscriber. On the other hand, if the subscriber uses a DSL connection, the billing of this kind of internet access appears to be usually a flat fee with a maximum of Mbytes of traffic per month. It is not longer necessary to record each connection to the Internet but to simply count the volume of the traffic. Of course it will be necessary to identify the subscriber of the fixed line on which the DSL connection has been activated. Those data are collected by the historical telecommunication operator for billing purpose. On top of that, there is the Internet provider who will offer Internet access by providing a unique IP address and the function of routing IP packets on the International Internet network.

What presents some doubts is the extension of the concept "data processed for the purpose of the conveyance of a communication on an electronic communications network", and more precisely "for the purpose of the conveyance of a communication". An interpretation *a contrario* could lead to the conclusion that any data which is not "necessary"[36] for

28 See Recital 42 of the Directive.
29 Art.2(b) of the Directive.
30 Art.5(1) of the Directive.
31 See Recitals 26 and 27 of the Directive.
32 Art.6(1) of the Directive.

33 See Article 29—Data Protection Working Party, *Privacy on the Internet. An integrated EU Approach to on-line data protection*, WP 37, November 21, 2000.
34 See Communication from the Commission to the Council and the European Parliament, *The Organisation and Management of the Internet. International and European Policy Issues 1998–2000*, Brussels, April 11, 2000, COM(2000) 202 final.
35 See Recitals 26 and 29 of the Directive. See also Article 29—Data Protection Working Party, *Opinion 1/2003 on storage of traffic data for billing purposes*, WP 69, January 29, 2003. In concordance with Article 5(1) "... This paragraph shall not prevent technical storage which is *necessary* for the conveyance of a communication without prejudice to the principle of confidentiality." See also Recitals 22, 26, 27, and 28 of the Directive.
36 In concordance with Art.5(1) "... This paragraph shall not prevent technical storage which is *necessary* for the conveyance of a communication without prejudice to the principle of confidentiality." See also Recitals 22, 26, 27, and 28 of the Directive.

the purpose of "conveyance" of communication ("*acheminement*" in French, "*conducción*" in Spanish) is not traffic data. For instance, the subject (title) of an email, its content, other data on logfiles like the navigator used, Accepted Language, Accepted Encoding, etc. is not traffic data.

## Retention of traffic data

The scope of rights of both Arts 5 and 6 can only be restricted, according to Art.15(1) if it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Member States may adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down above. All the measures referred to in this paragraph shall be in accordance with the principles of Community law, including those referred in Art.6(1) and (2) of the Treaty of the European Union.[37]

The principle of proportionality is a test created through the European Court of Human Rights case-law in order to evaluate the conformity of any restrictive measure applied to the fundamental rights guaranteed under the Convention.[38]

The protection of privacy is a fundamental right recognised in the Council of Europe conventions, EU legislation, and national constitutional traditions. Those principles have to be legally[39] balanced with other public policy objectives like the fight against cyber-crime, and the necessity to identify the liable person.

Especially after September 11, 2001,[40] a plethora of controversy has surrounded the retention of traffic data for security purposes. There are initiatives to extend the obligation to retain traffic data both at Community[41] and national[42] levels.

The Article 29 Data Protection Working Party has issued a document due to its concerns about certain proposals in the third pillar[43] of the EU that would result in the mandatory systematic retention of traffic data concerning all kind of communications for a period of one year or more for law-enforcement purposes. The Opinion says:

> "Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse. Systematic retention of all kinds of traffic data for a period of one year or more would be clearly disproportionate and therefore unacceptable in any case."[44]

37 Art.6 (ex Art.F) EUT (European Union Treaty).
"1. The Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law, principles which are common to the Member States.
2. The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community law."

38 Article 29—Data Protection Working Party, *Recommendation 3/97 on Anonymity on the Internet*, WP6, 3 December 1997, p.5.
See also: Article 29—Data Protection Working Party, *Recommendation 3/99 on The preservation of traffic data by Internet Service Providers for law enforcement purposes*, September 7, 1999.
Article 29—Data Protection Working Party, *Opinion 4/2001 on The Council of Europe's Draft Convention on Cyber-crime*, WP41, March 22, 2001.
Article 29—Data Protection Working Party, *Opinion 9/2001 on The Commission Communication on 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime*, WP51, November 5, 2001.

39 Following the second paragraph of Art.8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms: "in accordance with the law" and "necessary in a democratic society". See European Court of Human Rights, Case *Amann v Switzerland* (Application no.27798/95), Strasbourg, February 16, 2000; Case "*Rotaru v Romania*" (Application no.28341/95), Strasbourg, May 4, 2000; Case "*P.G. and J.H. v The United Kingdom*" (Application no.44787/98), Strasbourg, September 25, 2001.

40 See Art.29—Data Protection Working Party, *Opinion 10/2001 on The need for a balanced approach in the fight against terrorism*, WP53, December 14, 2001.

41 A Draft Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions (proposal for the Third Pillar legislation) was prepared recently by the Belgian government. The paper was leaked to a civil liberties organisation, Statewatch, who posted the draft on its website. The draft Framework Decision envisages the obligation to retain certain categories of "traffic data" (widening, indeed, its concept) for a period of 12 months minimum and 24 months maximum. (See *www.statewatch.org/news/2002/aug/05datafd.htl*, last visited October 31, 2002). See also Council of the European Union ("CEU"), 12198/01, Draft Reply to written question P-1887/01 put by Ilka Scröder on June 25, 2001 concerning "Enfopol 29 plans for retention of communication data", October 2, 2001; CEU, 10358/02, Note, "Draft Council conclusions on information technology-related measures concerning the investigation and prosecution of organised crime", June 24, 2002; CEU, 11490/02, Cover Note, "Questionnaire on traffic data retention", August 12, 2002; CEU, 12969/02, Preliminary draft reply to written question P-2503/02 put by Kathalijne Buitenweg on September 5,.2002 concerning "Proposal for a framework directive on data retention", October 11, 2002; The Danish Presidency, "Press release on the retention of traffic data", available at *www.eu2002.dk/news/news_read.asp?iInformationID=21663*, last visited October 31, 2002. The Danish Presidency, "Speaking notes concerning the Danish Presidency of the European Union. Police and judicial co-operation", available at: *www.eu2002.dk/news/upload/JSC20570200273162639.doc.*

42 In Belgium, the *Loi relative à la criminalité informatique* provides that telecommunication data has to be conserved (retention) for a period no inferior to 12 months: "... *ainsi que les obligations pour les opérateurs de réseaux de télécommunications et les fournisseurs de services de télécommunications d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, dans le cas à déterminer par arrêté royal délibéré en Conseil des ministres et sur proposition du ministére de la Justice et du ministre qui a les Télécommunications et les Entreprises et participations publiques dans ses attributions, les données d'appel de moyens de télécommunications. Ce délai, qui ne peut jamais être inférieur à 12 mois, ainsi que les données d'appel et d'identification seront déterminés par arrêté royal délibéré en Conseil des ministres et après avis de la Commission pour la protection de la vie privée.*" Secondary legislation will have to be passed in order to regulate this disposition. Art.14 of the *Loi du 28 novembre 2000 relative à la criminalité informatique.* Moniteur Belge, 03.02.2001. In France see *Loi sur la securité quotidienne.* Journal Officiel. n.266, November 16, 2001 p.18215. In Italy see Legge 15 dicembre 2001, n.438 *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2001*, n.374, *recante disposizioni urgenti per contrastare il terrorismo internazionale*, pubblicata sulla *Gazzetta Ufficiale* n.293 del 18 dicembre 2001. In Spain see Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico.* Boletín del Estado n.166, 12 de Julio de 2002.

43 See n.41 above.

44 Article 29—Data Protection Working Party, *Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff* (September 9–11, 2002) *on mandatory systematic retention of telecommunication traffic data*, WP64, October 1, 2002.

Both Directives 95/46 and 2002/58 are instruments regulating the protection of fundamental rights, so they determine the conditions to follow when restricting them, but not the restrictions themselves. It is for other kind of Conventions or laws to determine them. This is the case of the Council of Europe Convention on Cyber-crime[45] which determines that Parties shall adopt legislative measures to order a person to preserve and maintain[46] specified computer data,[47] including traffic data,[48] for a period of time as long as necessary, up to a maximum of 90 days.

The instruments regulating the period of retention and preservation of traffic should strictly follow the conditions established in fundamental rights norms since, as we have already mentioned, they constitute an exception to data protection rules, and exceptions has to be interpreted restrictively.

## Concluding Remarks

Even if internet was considered by the doctrine to be included in the regulation of Directive 97/66, the technology neutral approach of this new Directive is welcome since it removes any doubt and it also broadens the protection for future technology.

However, we can question the contribution of this new Directive to the protection of personal data in relationship with the general Directive. A *lex specialis* aims at particularising certain aspects of a *lex generalis* that need clarification in the practise, or due to their intrinsic characteristics need a more casuistic approach. On the one hand, we can see that several articles of the new Directive deal with principles already covered by the general Directive, which applied to the specific cases of electronic communications would have given the same result as those foreseen in the new Directive (security, confidentiality). On the other hand, controversial issues that would have needed a more precise and distinctive approach, due to the difficulty for the application of general principles, were left unspecified.

An example is Art.5(3). The first part is a pure application of Directive 95/46 principles. The second part does not properly address the particularities of the subject matter: "session cookies" present a clearly different nature and risk for the right to privacy and personal data protection *vis-à-vis* "permanent cookies". Nevertheless, this intrinsic difference is not transposed to the legislation since it is rather obscure what would be "strictly necessary in order to provide an information society service explicitly requested by the subscriber or user". Could we infer, in this case, that fundamental rights have been watered down in the name of technological neutrality?

Apart from that, consideration has to be given to the fact that in order to determine who are the data controllers concerned by this new Directive a functional analysis has to be made. We have seen that the narrow scope described in Art.3 does not represent the provisions of the Directive as a whole. The scope has to be interpreted together with other rules which describe activities regulated by the Directive, like the case of unsolicited communications, cookies, etc.

Certain initiatives at European level have shown the will to restrict the right to privacy as concerns the retention of traffic data. It is hoped that this restriction would only take place giving strict consideration to the conditions described in Art.15(1) and the supranational and international instruments protecting human rights.

45 Council of Europe. ETS No.185. Convention on Cybercrime. Budapest, November 23, 2001. Available at *http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.*

46 It is important to distinguish between "retention" and "preservation". The first one is made *ex ante*, that means systematically and during a certain period. It includes traffic data but not content data. The second one is made *ex post*, that is after a disputed event has happened, and includes content data.

47 The Convention on Cybercrime defines "computer data" as follows: Art.1(b) " . . . any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function."

48 The Convention on Cybercrime defines "traffic data" as follows: Art.1(d) " . . . any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."